

K&H Bank Zrt.

1051 Budapest, Vigadó tér 1.
Phone: (06 1) 328 9000, (06 30) 761 9000
Fax: (06 1) 328 9696
www.kh.hu • bank@kh.hu



GENERAL CONTRACTING TERMS AND CONDITIONS

FOR BANKING SERVICES REQUIRING ELECTRONIC AUTHENTICATION

Effective as of 11 July 2011



Company registration nr.: Cg. 01-10-041043 Budapest Meropolitan Court as Court of Registration



member of the KBC group

K&H Bank Zrt. (registered office: 1051 Budapest, Vigadó tér 1., company registration number: Cg. 01-10-041043, hereinafter: "Bank") shall provide Banking Services Requiring Electronic Authentication to its Clients in accordance with these General Contracting Terms and Conditions (hereinafter: "GCTC").

The personal scope of these GCTC shall extend to all persons using Banking Services Requiring Electronic Authentication as defined in Section 1 below.

- **The provisions of these GCTC shall apply:**

- to all Users using K&H e-banking services with a chip card who signed their contracts before or on 18 September 2009;
- to all Users using K&H e-banking services with SMS authentication who signed their contracts before or on 18 September 2009 and who are already using such services with the new electronic authentication process as per the notice sent by the Bank (K&H myID, e-PIN code, primary SMS password);
- to all Clients that have used the K&H Retail/SME/Corporate Telephone Banking Services actively as per the definition of the Bank (i.e. at least once since 1 January 2008) and that are now using them with the new electronic authentication process as per the notice sent by the Bank (K&H myID, e-PIN code);
- to all Clients not using the K&H Retail/SME/Corporate Telephone Banking Services actively that have switched to Banking Services Requiring Electronic Authentication as per the notice sent by the Bank (K&H myID, e-PIN code); and
- to all Clients having signed their contracts for Banking Services Requiring Electronic Authentication after 18 September 2009.



1. DEFINITIONS

1.1 Client: Natural persons over 18 years of age or, in the case of certain products, over 14 years of age; resident and non-resident legal or unincorporated entities; organisations (foundations, churches, associations, municipalities etc); businesses; or private individuals engaging in commercial activities that have a contract in place with the Bank for services provided by credit institutions to which the Banking Service Requiring Electronic Authentication apply.

1.2 Agent: A natural person identified by the Client in the Contract who can avail themselves to the services offered by the K&H Corporate Telephone Banking Service in the manner specified in the prevailing Announcement following a successful telephone authentication. Only a Client that is a resident or non-resident legal or unincorporated entity, organisation (foundation, church, association, municipality etc), business or private individual engaging in commercial activities may have an Agent.

1.3 Telephone Representative: A natural person identified by the Client in the Contract who liaises between the Bank and the Client in respect of the services available through the K&H Corporate Telephone Banking Service and acts on the Client's behalf and use the services defined in the prevailing Announcement following a successful telephone authentication. Only a Client that is a resident or non-resident legal or unincorporated entity, organisation (foundation, church, association, municipality etc), business or private individual engaging in commercial activities may have a Telephone Representative. The person of the Telephone Representative is not necessarily the same as the person with power of agency as defined in the relevant laws, i.e. the legal representative.

1.4 Signatory: A Telephone Representative identified by a Client that is a resident or non-resident legal or unincorporated entity, organisation (foundation, church, association, municipality etc), business or private individual engaging in commercial activities, who is also granted signatory powers and entitled to use the instruction type of services specified by the Client and defined in the prevailing Announcement following a successfully telephone authentication.

1.5 Transacting Person: A natural person identified by the Client in the Contract who can use the services available through the K&H SME Telephone Banking Service defined by the Client and specified in the relevant Announcement following a successful telephone authentication.

1.6 e-bank User: in the case of K&H corporate e-banking services, a natural person authorised by a resident or non-resident, legal or unincorporated entity, organisation, (foundation, church, association, municipality etc), business or private individual Client engaging in commercial activities to carry out electronic banking transactions in accordance with the terms and conditions applicable to the service.

1.7 electra User: A natural person authorized by a non-natural-person Client using Electra service in accordance with the terms and conditions applicable for this service for the execution of banking operations requiring electronic authentication appointed by the Client in the relevant Annex. We differentiate between electra Users having only querying powers and electra Users having other powers (i.e. signatory powers) granted based on the specified conditions.

1.8 e-box User: A User authorized – under the terms and conditions defined in the relevant Announcement – by a non-natural-person Client using the K&H e-box service in accordance with the terms and conditions applicable for this service for the execution of banking operations requiring electronic authentication through K&H e-box appointed by the Client in the relevant Annex. We differentiate between Normal Reeder and Confidential Reeder users. The powers relating to these roles are defined in the relevant Announcement.

1.9 User: a collective name for Clients, Permanent Proxies, Co-holders, Agents, Representatives, Signatories, Transacting Persons, Clients with a Query e-PIN and e-bank Users, electra Users and e-box Users.

1.10. Banking Services Requiring Electronic Authentication: a collective name for the services provided by the Bank and defined below:

- **K&H e-banking services:** banking services provided by the Bank and available to Clients online, i.e. the services available to Clients on the website of the Bank, <https://ebank.khb.hu/>. Natural person Clients must use the services themselves as they are not entitled to appoint a Permanent Proxy.
- **Electra service:** the name of the banking service provided by the Bank to non-natural-person Clients through an electronic system installed on the Client's computer suitable for the execution of the banking operations requiring electronic authentication specified in Section 13.5.10.
- **K&H e-box service:** electronic bank mailbox service provided by the Bank through the internet to Users of non-natural-person Clients through which Users may use the services specified in the Announcement.
- **K&H Retail Telephone Banking Service:** telephone banking services provided by the Bank to natural person Clients. A Permanent Proxy or a Co-holder may act in the Client's place or on their behalf if necessary, using their personal K&H myID and e-PIN code.
- **K&H SME/Corporate Telephone Banking Service:** telephone banking services provided by the Bank to non-natural-person Clients. These services differ in their scope, which is defined in the relevant prevailing Announcement.

1.11. K&H myID: The eight-digit numeric identification code defined in the manner described in Section 3 for the unique identification of the User in Banking Services Requiring Electronic Authentication.

1.12. e-PIN code: The secret six-digit numeric identification code defined in the manner described in Section 4 which, together with the K&H myID, serves to uniquely identify the User in Banking Services Requiring Electronic Authentication.

1.13. Queriable e-PIN code: The e-PIN code given to an SME Client, to be used for the services specified in the relevant Announcement. The e-PIN code is not allocated to a single natural person; the Client may disclose it to others at their responsibility.

1.14. Electronic authentication:

- Identification with K&H myID: For the use of Banking Services Requiring Electronic Authentication without a chip card; to be used together with the e-PIN code or, in the case of K&H e-banking requiring SMS authentication or in the case of K&H e-box service, the primary SMS password.
- Identification with a chip card: e-bank Users may opt to identify themselves with the help of a chip card authentication tool when using K&H e-banking services or jointly using K&H e-bank and K&H e-box services, in which case the Bank shall provide a chip card and a chip card reader to them. In order to use the services, Users must authenticate themselves with their chip card together with the matching PIN code.
- Identification with Token: For the use of the Electra service or the joint use of the Electra service and the K&H e-box service, the Bank provides electra Users with an authentication tool, a Token. In order to use the service(s), Users must authenticate themselves with their Token together with the matching Token password.

1.15. Contract: a unique Contract made by and between the Client and the Bank for the use of Banking Services Requiring Electronic Authentication. Its annexes (hereinafter: the Annex), this GCTC and the General Terms and Conditions of the Bank and the relevant Announcements form an integral part thereof.

1.16. Announcements: Notices displayed in the public areas and on the website of the Bank setting out the terms and conditions of using Banking Services Requiring Electronic Authentication pursuant to these GCTC.

Among others, Announcements describe the contents of the relevant services, the specification of the tools required for their use and the applicable fees and charges.

1.17. Definitions pertaining to the K&H e-banking services:

Chip card: a plastic card issued by the Bank and not regarded as a bank card. Acting as an electronic means of payment providing remote access, the card and its matching PIN code allow the given User to use both the K&H e-bank service and the K&H e-box service through the internet. The chip card issued by the Bank is the property of the Bank. Only natural persons may hold chip cards. One natural person may only have one chip card at a time.

Chip card PIN code: a secret numeric identification code generated by the Bank during the process of chip card authentication, required for the use of K&H e-banking/K&H e-box services. The PIN-code of the chip card is different from the e-PIN code.

Primary SMS password: One-time password sent by the Bank to the Client in an SMS message upon login.

Secondary SME password: (mTAN): It is used by online banking services as an SMS containing unique one-time passwords, enabling the user to authorize financial transactions. The password is sent by the Bank to the Client in an SMS when a given operation is to be performed, in case of each transaction initiated by the Client.

Electronic banking action: Any and all queries, orders and notifications given by the Client to the Bank at least partially in the form of electronic signals via direct computerised communication. In electronic banking actions the User's signature is substituted with an identification code given in the format approved by the Bank.

Access right: A right bestowed upon the e-bank User by the Client, granting the e-bank User corporate signatory powers in respect of all the existing and future accounts of the Client included in the K&H corporate e-banking services. The Client grants access rights to e-bank Users in the relevant Annex of the Contract.

Driver: The program required for the operation of the chip card reader.

Minimum configuration: The minimum technical conditions required for the use of the service.

Operation in public places: Operation in any places other than the computer of the Bank or the User.

Chip card reader: A technical tool required for the use of the K&H e-banking services requiring chip card authentication.

1.18. Definition pertaining to Electra services:

Token: A physical storage device issued by the Bank, which together with its matching Token password allows the given Token holder User to use the Electra service. The Token issued by the bank is the property of the Bank. Only natural persons may be holders of a Token. One natural person may only have one Token at a time.

Token password: An 8-character identification code specified by the User at the time of the first login using the Token, which has a dual function. It shall be used on the one hand at the time of each login during the use of the Electra service and on the other hand, for the approval of Electronic Banking Operations performed under the Electra service (by electra Users to whom signature rights were granted using the form provided in the relevant Annex).

Electra System: The Bank's electronic system for the execution of Banking Operations Requiring Electronic Authentication available under the Bank's Electra service.

Electra Software: Any and all of the computer programs, which allow the electra User the execution of Electronic Banking Operations – and thereby the use of the Bank's services.

Elektra Software Module: All of the services requested by the Client and set by the Bank from the ones listed in Section 13.5.10.

Electronic Banking Operation: All orders and notices provided to the Bank by the electra User directly through



the application of computer communication, at least partly in the form of electronic signals. During Electronic Banking Operations the electra User supplements his signature by personal identification coding in the form approved by the Bank or the use of another similar authorization tool (approved by the Bank). Orders and notices provided as Electronic Banking Operations are irrecoverable and non-modifiable unless agreed otherwise between the Parties.

1.19. Definitions pertaining to K&H e-box services:

Token: A physical storage device issued by the Bank, which together with its matching Token password allows the given Token holder User to use the K&H e-box service. The Token issued by the bank is the property of the Bank. Only natural persons may be holders of a Token. One natural person may only have one Token at a time.

Token password: An 8-character identification code specified by the User at the time of the first login using the Token, which shall be used at the time of each login during the use of the K&H e-box service.

Chip card: a plastic card issued by the Bank and not regarded as a bank card. Acting as an electronic means of payment providing remote access, the card and its matching PIN code allow the given User to use both the K&H e-bank service and the K&H e-box service through the internet. The chip card issued by the Bank is the property of the Bank. Only natural persons may hold chip cards. One natural person may only have one chip card at a time.

Chip card PIN code: a secret numeric identification code generated by the Bank during the process of chip card authentication, required for the use of K&H e-banking/K&H e-box services. The PIN-code of the chip card is different from the e-PIN code.

Primary SMS password: One-time password sent by the Bank to the User in an SMS message upon login in accordance with the provisions of Section 6.8.

Electronic Banking Operation: All queries, orders and notices provided to the Bank by the User directly through the application of computer communication, at least partly in the form of electronic signals. During Electronic Banking Operations the electra User supplements his signature by personal identification coding in the form approved by the Bank.

Access right: The right granted by the Client to the e-box User on the basis of which the e-box user disposes of the account or accounts specified by the Client and is authorized to perform Electronic Banking Operations. The Client specifies the access rights of e-box Users for the Bank using the form provided in the relevant Annex.

2. GENERAL PROVISIONS

2.1. Clients can request Banking Services Requiring Electronic Authentication in a Contract signed with the Bank for this purpose, under which Users may use the banking services specified in the Announcement pertaining to the selected electronic channel, using their K&H myID. The Bank issues a K&H myID, an e-PIN code and a K&H e-bank chip card and a matching PIN code or an SMS password to be used for the services.

2.2. Issues not regulated in these GCTC shall be governed by the provisions of the General Terms and Conditions of the Bank and the General Contracting Terms and Conditions applicable to the services used by the User. Furthermore issues not addressed herein shall be subject to the provisions of the Civil Code and the prevailing legislation on credit institutions, payments and electronic payment channels. In addition, the User expressly confirms and accepts the provisions set out in Section 4 Data protection, data handling and the provision of information and grants the Bank the powers described to therein.

2.3. The use of the services is subject to the fees, commissions and charges set out in the relevant Announcements. The Bank shall be entitled to charge to the Client's account the fees, commissions and charges at the time specified in the relevant Announcements. The fees, commissions and charges payable for the Banking Services Requiring Electronic Authentication quoted in the relevant Announcements do not include the fees, commissions and charges payable on the transactions effected while using the services. The costs associated with the use of the tools required for the use of the Banking Services Requiring Electronic Authentication (telephone, internet etc) shall not be payable by the Bank.

2.4. When a User is initiating an order or executing a banking transaction, the time when the service was requested shall be the time determined and recorded by the electronic system of the Bank. The Bank shall execute the orders generated via the Banking Services Requiring Electronic Authentication within the timeframe specified in the relevant Announcements concerning the procedures of receiving and executing Orders.

2.5. The Client shall honour their payment obligations to the Bank arising under these GCTC as they become due/as they occur. The Bank shall have the right to charge any amounts receivable from the Client to any of their accounts managed by the Bank, or to offset such amounts against any amounts due to the Client on another account or from the Bank.

2.6. The Client undertakes to pass on the contents of the GCTC to the User identified by them during the use of the service .

2.7. Each User shall have their unique K&H myID, which can only be used by them. Users shall be bound by the obligations of the Client set out in the GCTC.

2.8. The User shall acknowledge the instructions given while using the service as per the GCTC following the identification procedure as their own, and they shall take full responsibility for such instructions.

2.9. The Bank does not provide investment advice regarding orders given via Banking Services Requiring Electronic Authentication, thus the Bank does not consider the suitability and appropriateness of the product in question for the Client.

2.10. Banking Services Requiring Electronic Authentication are provided in the Hungarian language. The User can only give orders in other languages on their own responsibility.

3. COMPOSITION AND GRANTING OF A K&H MYID

3.1. All new Users shall receive their own K&H myID from the Bank. Natural persons may obtain their new K&H myID in a branch or via the K&H Retail Telephone Banking Service, while legal and unincorporated entities may obtain their new K&H myID in a branch only.

4. COMPOSITION AND GRANTING OF THE E-PIN CODE

4.1. All new Users falling shall receive their own e-PIN code. The e-PIN code can be set up in a branch as a series of numbers determined by the User or generated in advance by the Bank. The latter type can also be mailed to the User. (For details see the effective Announcement).

5. ACCESS TO AND MODIFICATION OF BANKING SERVICES REQUIRING ELECTRONIC AUTHENTICATION

5.1. The Client shall specify the Banking Service(s) Requiring Electronic Authentication they wish to use in the relevant Annex to the Contract, then the Bank shall grant access to the User thereto.



5.2. The Bank shall provide the K&H myID to the User after the signature of the Contract. The Bank shall be entitled to withhold the K&H myID, the e-PIN code and the chip card until the Client has complied with all terms and conditions of requesting the services in question or putting the authorisation into effect and any other terms and conditions set out in the Contract.

5.3. The User shall be entitled to change their personal e-PIN code in the automated telephone system or in the e-banking application. The chip card PIN code can be changed in the e-banking application.

5.4. The User shall be responsible for their K&H myID and e-PIN code and their chip card and matching PIN code from their receipt or creation in the system.

6. PROCEDURES TO BE FOLLOWED BY THE USER; ELECTRONIC AUTHENTICATION

6.1. If the User fails to comply with all the rules and requirements applicable to Electronic authentication and set out herein, the Bank shall be entitled to refuse to provide the requested service.

6.2. Prior to their electronic authentication Users can only carry out transactions which are not subject thereto according to the relevant Announcement.

6.3. Users must enter their K&H myID and e-PIN code when using Banking Services Requiring Electronic Authentication; their primary/secondary SMS password when using K&H e-banking or K&H e-box services requiring SMS authentication; their chip card and matching PIN code when using K&H e-banking services or jointly using K&H e-banking and K&H e-box services requiring chip card authentication; and their Token and matching Token password when using the Electra service or K&H e-box service requiring Token authentication.

6.4. The handling of e-PIN codes and PIN codes by the Bank is subject to strict security requirements.

6.5. Identification on landline or mobile telephone (K&H Retail Telephone Banking Service, K&H SME Telephone Banking Service, and K&H Corporate Telephone Banking Service):

Having successfully reached the relevant telephone banking service, the User must enter their K&H myID code and their e-PIN code on a touch tone or mobile telephone. Once they have been successfully identified, they are put through to the automated system or a Telephone Banker or a staff of the K&H Corporate Telephone Banking Service who will assist them with the execution of their order.

6.6. Online authentication for K&H e-banking services:

- Accessing the K&H e-banking services with SMS authentication: the User keys in their K&H myID and e-PIN code using the keyboard. The Bank sends them the primary SMS password to their mobile phone. Only when all three codes have been entered can the User use the K&H e-banking services.
- Accessing K&H e-banking services with the chip card: the User inserts the chip card in the chip card reader according to instructions and then keys in their PIN code. The services will be accessible after a successful authentication of the correctly entered code.

6.7. Authentication for Electra services:

After the insertion according to the instruction of the Token in the USB connector, the electra User keys in the Token password using the keyboard. The authentication is successful and the Electra service is accessible after the correct entry of the Token password.

6.8. Authentication for K&H e-box services:

- The e-bank User using K&H e-banking services may access the K&H e-box service after accessing the e-bank as described in Section 6.6.

- Accessing the K&H e-box service with SMS authentication: the e-box User keys in their K&H myID and e-PIN code using the keyboard. The Bank sends them the primary SMS password to their mobile phone. Only when all three codes have been entered can the User use the K&H e-box service.
- Accessing the K&H e-box service with the chip card: the e-bank User inserts the chip card in the chip card reader according to instructions and then keys in their PIN code. The K&H e-bank and the K&H e-box services will be accessible after a successful authentication of the correctly entered code.
- Accessing the K&H e-box service with the Token: After the insertion according to the instruction of the Token in the USB connector, the e-box User keys in the Token password using the keyboard. The authentication is successful and the e-box service is accessible after the correct entry of the Token password.

7. GENERAL RIGHTS AND OBLIGATIONS OF THE PARTIES

7.1. The User shall always act during the term of the Contract signed with the Bank as can be reasonably expected in such circumstances. This includes an obligation to retain their K&H myID and e-PIN code and the chip card and PIN code required for their authentication and, together with their primary/secondary SMS password, keep them confidential. If the User records their K&H myID and e-PIN code or their primary/secondary SMS password and the PIN code for their chip card, they shall keep such records separate from any and all documents associated in any way with their bank accounts or their chip card, and they shall seek to ensure that they cannot be accessed and acquired by third persons. The User shall be responsible for the safe handling and the proper and lawful use of their chip card, chip card reader, K&H myID and PIN codes. The User shall be fully liable for any damages resulting from their failure to comply with the above fully or in part. Furthermore the User shall be liable for any direct and consequential damages resulting from the incorrect use of their K&H myID, e-PIN code, primary/secondary SMS password, chip card, chip card PIN code and chip card reader or their acquisition by third persons. The Bank shall accept no liability for any damages resulting from the circumstances described herein.

7.2. The Bank shall use all reasonable efforts in its electronic data transmission to ensure that the Client's details cannot be accessed by unauthorised persons. The Client acknowledges that the Bank shall not be liable for any damages arising from data becoming accessible by a third person despite the Bank's reasonable efforts to prevent this.

7.3. In the case of K&H e-banking and K&H e-box services requiring SMS authentication the liability of the Bank shall extend from sending the message from the Bank through to its arrival to the message centre of the relevant mobile network operator.

7.4. Irrespective of the User's liability stipulated in Section 7.1 the Bank, in accordance with its statutory obligation, must refuse to provide the relevant service if it discovers that the User's K&H myID, e-PIN code, primary/secondary SMS password or chip card and chip card PIN code has been lost by or stolen from the User. The Bank must prohibit the provision of services requested in this manner at the time and thereafter, to delete the e-PIN code and cancel the chip card, and to promptly notify the Client thereof in the most practicable manner, in most cases by telephone or, if that fails, by e-mail, fax or post.

7.5. The Bank shall be entitled to refuse to execute a User's order if it does not comply with the legislative provisions in effect, is incomplete, incorrect or contains other incorrect data, and at the same time it shall inform the User of the reason(s) thereof. The Bank shall not be responsible for events and non-performances arising from the fact that the User fails to use their K&H myID, chip card and chip card reader altogether or use them incorrectly or not in the environment required for their correct use. Environment for correct use shall

mean the tools specified in these GCTC, the components of the installation program provided by the Bank and the technical environment suitable for their regular use at the time.

7.6. The Bank shall accept and handle the orders received via the system for Banking Services Requiring Electronic Authentication and record them in its computerised system if they meet the same requirements in terms of their content as orders given in writing. The recorded entry substitutes the written order and it is the equal thereof in every respect. The Client shall accept the data recorded in the system of the Bank as authentic and recognise them as evidence of both giving and executing the order in the event of a legal dispute.

7.7. In the case of services used according to the GCTC the User shall recognise the information provided after the authentication as their own and they shall take full liability therefor.

7.8. The Bank shall be entitled to refuse to execute orders if a technical error occurred during their entry and the User did not confirm the order and/or its execution as a result.

7.9. The Bank shall not be liable for any technical errors occurring during the provision of the services or the failure of transactions resulting therefrom if such errors occurred outside the control of the Bank or cannot be attributed thereto.

7.10. Users must give their K&H myID and e-PIN code, or their primary/secondary SMS password, or their chip card and their chip card PIN code together to prove that they are authorised to give instructions and orders using Banking Services Requiring Electronic Authentication. The Bank shall not check the User's authority for and the circumstances of their use of the K&H myID and the e-PIN code, or the SMS password, or the chip card and the chip card PIN code. The Bank shall not be liable for any damages arising from the unauthorised use thereof. However, the Client acknowledges that the Bank is entitled to check the legitimacy and authenticity of orders received through the use of these services.

7.11. The Client shall ensure that the funds required for the execution of their order are available at the time, including any and all fees and charges applicable to the execution of such orders at the time, which are due on their performance. If the funds on the Client's account do not fully cover such fees and charges, the Bank shall be entitled to refuse to execute the relevant order. The Bank may limit the number of orders and that can be placed using the K&H myID in a specific period of time and the sum thereof. The Bank shall inform the User about these limits in the relevant parts of the Announcement.

7.12. The User cannot withdraw any orders given via electronic authentication, except in the cases specified in the Announcement. The Bank shall be entitled to charge to the Client's account the amounts specified in the orders given in accordance with the GCTC during the electronic authentication using the Banking Services Requiring Electronic Authentication.

7.13. The Client shall be informed about the transactions performed during the use of such services in the bank account statement. The Client shall immediately report to the Bank any unauthorised actions discovered in their bank account statement. However, such complaint shall not authorise the Client to delay the performance of any of its obligations to the Bank. Such complaints can be made by telephone, in writing (sent to the addresses stated in the Announcement) or in person in any branch of the Bank.

7.14. The Bank shall not be liable for any damages arising within the control of the operators or in the use of telephone lines, private switchboards and computerised systems, or the use of telephone sets or computers used by the User. Furthermore the Bank shall not be liable for any damages arising from the use of intercepted information obtained by unauthorised access to telephone sets, telephone lines and computerised electronic systems. The User hereby irrevocably exempts the Bank from any liability that may result from a telephone conversation being cut off, repeated or distorted, or from an error in the computerised system or computer network or a disruption of their operation for whatever reason.



8. DELETION OF E-PIN CODE, DELETION OF CHIP CARD

8.1. The User shall immediately report to the Bank if he discovers that

- their e-PIN code, primary/secondary SMS password, or chip card and PIN code has been lost or stolen;
- their e-PIN code, primary/secondary SMS password or chip card PIN code has been acquired by a third person; or
- an unauthorised transaction has been initiated using their e-PIN code or their chip card.

8.2. Users may make such reports in writing, in any branch of the Bank or by telephone to the relevant telephone banking service; all telephone banking services can be contacted twenty-four hours, seven days a week regarding the deletion of e-PIN codes and the cancelling of chip cards. Such reports can only be made by Users and e-PIN codes can be deleted and chip cards can only be cancelled by the Bank. The Bank will also accept such a report from another person if the relevant User is not in a position to do so and the person making the report can only assume this circumstance. In this case the person making the report must give their personal identification details (name, address, mother's name) and must assert that they are expressly requesting the deletion of the PIN code or the cancelling of the chip card. The Bank shall not examine actual authority when the report is made, and it shall not be liable for any damages arising from unauthorised reports.

8.3. The report shall include:

- If made by a natural person: the User's personal identification details (name, address, mother's name, any identification number used in banking except for a bank account number). If the User fails to comply with this requirement, the Bank may refuse to record their report and simultaneously inform the User thereof.
- If made by a legal or unincorporated entity: the details of the legal or unincorporated entity Client (name, registered office) and the User's personal identification details (name, address, mother's name, bank identification number).

When reporting such an incident – in the event of the deletion or cancellation of an e-PIN code, primary/secondary SMS password or chip card PIN code due to their acquisition by an unauthorised person – the event prompting the report must be specified together with its venue and timing or, if the User does not know the exact details, its likely venue and timing. If the report does not contain the User's personal identification details, the Bank may disregard it and immediately inform the User thereof. The Bank shall have the right to request further details related to the User and kept on file by the Bank in order to verify the User's authority for making such a report. The reports shall also serve as an instruction to delete the relevant e-PIN code or to cancel the relevant chip card. The Client shall be liable for any and all damages arising between the time the Client learns about the facts serving as a basis for the report and the time when the report is made to the Bank. If the reason of the report made in order to have an e-PIN code deleted or a chip card cancelled is an action assumed to have been unauthorised and discovered on a bank account statement or on the account and the User does not request the deletion or cancelling when making the report, the Bank shall act in accordance with the rules applicable to complaints. If a reasonably careful analysis of the facts concludes that the reported event(s) occurred in a criminal offence, the Client shall immediately report this suspicion to the relevant authorities.

8.4. Other than that, any third persons having discovered that the e-PIN code or chip card of their holder has been lost or stolen may report this in any of the manners listed in Section 8.2. Persons making such a report must give their personal details (name, address, mother's name) and the details of the chip card in question in a clearly identifiable way, and explain how they learnt about the loss or theft. If the chip card cannot be clearly identified on the basis of the report, the Bank will disregard the report and refuse the deletion/cancellation. Reports described herein shall also be governed by the other provisions of Section 8.

8.5. The local time in Hungary as measured and recorded by the central systems of the Bank shall be used to determine the time of the report, the deletion of the e-PIN code and the cancellation of the chip card as well as the liability for costs, risks and damages.

8.6. Based on the report received, the Bank shall immediately proceed to delete the e-PIN code/cancel the chip card. The deletion/cancellation shall come into effect when the Bank has taken the required actions in the time needed therefor. Upon the deletion of the e-PIN code all Banking Services Requiring Electronic Authentication through the e-PIN code shall immediately become unavailable to the User.

8.7. The Bank may charge a fee for deleting the e-PIN code/cancellation the chip card. The rate of this fee is quoted in the prevailing Announcement. Such a report shall not authorise the Client to delay the performance of any of its obligations to the Bank.

8.8. The deletion of the e-PIN code/cancellation of the chip card shall be final and irrevocable; neither the e-PIN code, nor the chip card can be used thereafter. Deleted e-PIN codes and cancelled chip cards cannot be used even if they are subsequently found. The risk of deletion/cancellation and any damages arising therefrom (from the fact that the deleted e-PIN code/cancelled chip card cannot be used) shall be borne by the Client. The Bank shall not be liable for any damages suffered by the Client or any third parties as a result of a failure to delete the e-PIN code/cancel the chip card or an abuse of their deletion/cancellation. E-PIN codes/chip cards can only be replaced with a new e-PIN code/chip card.

8.9. For security reasons the Bank shall have the right to delete the e-PIN code/cancel the chip card if the risk arising from the relevant Contract significantly changes; if there are insufficient funds on the account, if there are reasonable grounds for suspecting that the code has been abused or used irregularly; if the is found to be in material breach of contract; or if the contract ceases to exist. The Bank shall inform the User of the deletion of their e-PIN code or the cancelling of their chip card.

8.10. The User accepts that the Bank shall block their e-PIN code (for 24 hours) if they enter it incorrectly three times in succession when using any of the Banking Services Requiring Electronic Authentication and block their chip card. If an e-PIN code is blocked three times within 30 calendar months, it shall be deleted finally and irrevocably.

- Blocking and deletion of the e-PIN code: the Bank shall block e-PIN code (for 24 hours) if it is entered incorrectly three times in succession. If an e-PIN code is blocked three times within 30 calendar months, it shall be deleted finally and irrevocably.
- Blocking of the chip card: the Bank shall block the chip card after the chip card PIN code is entered incorrectly three times in succession. The blocked chip card can only be released by the Bank and involves replacing it with a new card when the original card is handed in. The fee payable for unblocking the chip card is quoted in the relevant Announcement.
- Blocking of Token: the Bank shall block the Token after the Token password is entered incorrectly five times in succession. The blocked Token can only be released by the Bank after an identified phone-call to the Corporate Telephone Banking Service.

9. RULES APPLICABLE TO LIABILITY FOR DAMAGES RESULTING FROM THE DELETION OF THE E-PIN CODE/CANCELLATION OF THE CHIP CARD

9.1. The risk of the deletion of the e-PIN code/cancellation of the chip card and any damages arising therefrom shall be borne by the Client. The Bank shall not be liable for any damages suffered by the Client or any third parties resulting from the failure to delete the e-PIN code/cancel the chip card or from any abuse related to the deletion/cancellation, or arising subsequently in connection therewith.

9.2. The Bank only take responsibility for damages arising within the control of the Client following the deletion of the e-PIN code/cancellation of the chip card if the damages in question are expressly attributable to the negligent conduct of the Bank. The Bank shall be exempted from liability if it successfully proves that the damages occurred due to a breach of contract wilfully committed by the User or caused by their gross negligence. Any and all risks and costs associated with banking actions requiring the simultaneous use of the chip card and chip card PIN code, the K&H myID and the e-PIN code and the primary/secondary SMS password shall be borne by the Client as damages arising from their wilful conduct or gross negligence.

10. AMENDMENT OF THE TERMS OF THE CONTRACT

10.1. The Bank shall expressly reserve and the Client shall acknowledge the right to supplement the provisions of the GCTC whenever new or improved services are introduced, and to unilaterally amend the provisions of the GCTC in force and the terms and conditions set out in the Announcement to reflect any changes in the legislation applicable or relevant to the activities and the operating conditions of the Bank; in the rulings of the Central Bank of Hungary or any other regulations binding on the Bank, the Central Bank base rate or any other Central Bank interest rates; in the opportunities for fundraising in money markets and the costs thereof; in other prime costs of the Bank, the consumer price index or state interest subsidies; in taxes and contributions, the reserve requirements or the procedures or operating processes of the Bank, and in the risk associated with a service or the Client.

Should the Bank modify the provisions of its effective General Contracting Terms and Conditions and/or relevant Announcement to the detriment of the Client, it shall be obliged to display such amended General Contracting Terms and Conditions and/or Announcement in its branches and to publish them on its website 15 days before the modification is to take effect. Should the Client not agree with such a modification, they shall have the right to terminate the contract within 15 days of the publication of the new terms, or else the modification will take effect and become applicable to the Client.

11. BANK ACCOUNT STATEMENT AND OTHER DOCUMENTS

11.1. Notices about orders given by the User in accordance with the terms and conditions of this contract shall only be sent by the Bank if specifically requested by the Client. Such special notices shall be subject to a charge published in the prevailing relevant Announcements.

11.2. The document received about the service(s) used (bank account statement, special notice) shall be regarded as written proof of the execution of such orders.

12. TERMINATION OF BANKING SERVICES REQUIRING ELECTRONIC AUTHENTICATION

12.1. The Contract may cease to exist :

- (a) by extraordinary termination by the Bank with immediate effect;
- (b) by regular termination by the Bank or the Client;
- (c) by mutual consent on a date agreed by the Bank and the Client;
- (d) if the Client ceases to use all Banking Services Requiring Electronic Authentication; or
- (f) if all bank account contracts serving as a basis for the service cease to exist for whatever reason.

12.2. In the event of a material breach of contract by the Client the Bank shall have the right to terminate the contract with immediate effect and at the same time to terminate the User's access right to the service (extraordinary termination).

12.3. The Bank has the right to terminate the Contract without an explanation, with a notice period of 30 calendar days (regular termination). The Client has the right to terminate the Contract at any time with regular

termination with a notice period of 30 calendar days, provided that they have complied with all of their outstanding payment obligations.

12.4. Upon the cessation of the Contract – if a K&H e-banking service requiring chip card authentication is set up within the framework of the Banking Services Requiring Electronic Authentication – the User shall return the chip card and the chip card reader provided by the Bank within 15 calendar days therefrom, provided that they do not use any other Banking Services Requiring Electronic Authentication. Any and all damages resulting from the failure of the Client to do so shall be borne by the Client. If the User fails to return the chip card reader upon the cessation of the Contract or returns it late or damaged beyond reasonable wear and tear, they shall pay the fee of the chip card reader to the Bank. If the User fails to do so in time or at all, the Bank shall be entitled to collect the fee of the chip card immediately from the Client. The fee of the chip card reader is stated in the Announcement.

12.5. Upon the cessation of the Contract for whatever reason the access right granted to the Client and all Users under the Contract in question shall also cease to exist and consequently the Client and the Users will no longer be able to use the relevant services.

12.6. The cessation of the Contract for whatever reason shall not affect the other contract(s) of the Client with the Bank.

13. OTHER SPECIAL PROVISIONS APPLICABLE TO THE VARIOUS BANKING SERVICES REQUIRING ELECTRONIC AUTHENTICATION

For the matters concerning various Banking Services Requiring Electronic Authentication not regulated in this Section, the general provisions of the GCTC shall apply.

13.1. OTHER SPECIAL PROVISIONS APPLICABLE TO K&H E-BANKING SERVICES

13.1.1. K&H e-banking services can be used by Clients that have the appropriate, valid and effective contracts for account opening and management in place with the Bank, and that have the hardware and software required for the services (see the User Guide for their list). In the case of a Joint Account as defined in the “General Contracting Terms and Conditions for Bank Account, Deposit Account and Term Deposit Products Provided to Resident and Non-resident Natural Persons”, the K&H e-banking service may only be used by the natural person specified as an “Accountholder” in the bank account agreement and may not be used by the “Co-Accountholder”.

13.1.2. The e-bank User must have the equipment required for the use of the K&H e-banking services and specified by the Bank, and must be authorised for their use. The e-bank User must familiarise themselves with the technical attributes of this equipment and any other tools required for the use of the services.

13.1.3. The Bank shall provide the e-bank User with the tools and equipment required for the use of the services: the chip card and the chip card reader (the property of the Bank) and the installation guide demonstrating their use. The chip card reader a Bank is the property of the Bank and the e-bank User as its holder shall only be given it for use. The user manual and the installation guide for the services and the driver for the chip card reader can be downloaded from <https://ebank.khb.hu/>. The Bank reserves the right to update and supplement the user manual from time to time in order to improve the quality of the service. The update of the user manual shall not require the amendment of the Contract under any circumstances, and the Bank shall inform e-bank Users thereof electronically using the e-banking application.

13.1.4. The e-bank User may collect their chip card immediately after the signature of the Contract in any branch of the Bank. The Bank hereby points out to the e-bank User that, should it not have a chip card to give to the e-bank User for reasons beyond its control, it shall inform the e-bank User about the date by which it will be able do so when they come to collect it.



13.1.5. The Bank as the owner of the driver required for the chip card reader grants non-exclusive and non-unrestricted right to the e-bank User to use the chip card reader. Only the e-bank User is authorised to use the chip card reader driver on the specified hardware and software configuration under this right for the normal use of the service, in accordance with the relevant provisions.

13.1.6. This right shall not extend to reproduction, reworking, processing and translation, including any other modifications and the reproduction of the result thereof and the preparation of backup copies.

13.1.7. The Bank hereby declares and warrants that the chip card and chip card reader provided to the e-bank User and the driver required for the use of the chip card reader and downloadable from the internet are free from litigation, encumbrances and claims, and no third parties have any rights that would limit the Client in exercising their own rights pertaining thereto or prevent them from doing so. The Bank hereby declares and warrants that the chip card, the chip card reader and the driver required for the chip card reader meet the specification provided by the Bank at the time of their delivery/download, and that they can be used normally on the specified hardware and software configuration.

13.1.8. The obligations of the Bank shall extend to the following:

- (a) advice provided on the user of the chip card and the chip card reader and the installation of the driver for the chip card reader;
- (b) troubleshooting advice;
- (c) investigation of problem reports.

13.1.9. Furthermore, under the warranty the Bank undertakes to replace faulty chip cards and chip card readers free of charge. However, if such a fault is attributable to their abnormal use by the e-bank User, the Bank shall charge the fee quoted in the Announcement for this service.

13.1.10. The warranty provided by the Bank as per the above shall not extend to the own hardware peripherals of the Client and any software installed thereon or connected thereto; the Bank shall accept no liability for damages resulting therefrom.

13.1.11. The Bank shall not be held liable for damages attributable to malware/spyware programs outside its information technology structure. Furthermore the Bank shall accept no liability for damages arising from the lack of proper protection (anti-virus and anti-spyware programs) of the User's own information technology tools and equipment.

13.1.12. The Bank shall be entitled to use the assistance of specialist third persons in order to comply with its obligations under the warranty.

13.1.13. As a condition precedent to the warranty service, the Client undertakes to provide access to the chip card, the chip card reader, the chip card reader driver and the hardware accommodating it, and to make these available to the Bank with the conditions requested by the Bank and for the duration required for the delivery of the warranty service.

13.1.14. The validity of the chip card is visibly stated on it in a month/year format, and it shall be valid until 24.00 hrs on the last day of the relevant month.

13.1.15. The e-bank User shall use the chip card reader and the chip card provided by the Bank normally and to keep them undamaged. The Client shall immediately inform the Bank if the chip card reader gets damaged, faulty, lost or stolen, and of any other events concerning the chip card reader. The Client shall be liable for damages occurring in the chip card reader to the Bank as per the Announcement. The e-bank User shall use the chip card reader and the chip card in accordance with the installation guide provided by the Bank, and to observe the requirements set out therein.

13.1.16. The Bank reserves the right to stipulate further requirements concerning the use of the chip card reader in the relevant Announcement.

13.1.17. The chip card can only be used by the e-bank User, and it cannot be transferred, pledged as collateral or deposited as security. Legal and unincorporated entity Clients must notify the Bank when its relationship with

an e-bank User is terminated in this capacity. E-bank Users must have their e-PIN code deleted and their chip card cancelled if they have no access to other Banking Services Requiring Electronic Authentication.

13.1.18. If the Client is a K&H Trambulin 14+ account holder and a minor, then their valid use of the K&H Trambulin e-banking services shall be subject to the written consent of and an absolute guarantee by their legal representative.

13.1.19. In the case of K&H corporate e-banking services the Client shall decide at their sole discretion and responsibility to which person(s) to grant an access right. Only the e-bank Users registered by the Client according to the relevant provision as lawful e-bank Users shall be regarded as such by the Bank.

13.1.20. Based on the information provided by the Client, the Bank shall set up the e-bank User's access right and manufacture the chip card to be delivered to the relevant e-bank User in person.

13.1.21. The e-bank User holding a valid chip card and entering the chip card PIN code, K&H myID, e-PIN code and primary/secondary SMS password shall have corporate signatory powers within the scope in K&H corporate e-banking services and in respect of all the existing and future accounts of the Client included therein

13.1.22. The Client may use the relevant Annex to the Contract for notices concerning granting access rights to e-bank Users and deleting them, and modifications in user details.

13.1.23. Each e-bank User of the K&H corporate e-banking services must have at least one chip card.

13.1.24. The Bank shall enclose a PIN code to the chip card, which will be delivered to the Client in a sealed envelope. The Bank shall deliver the chip card and the PIN envelope only to the e-bank User; it shall not accept a power of attorney on delivery. When delivered the chip card, the e-bank User shall confirm on the receipt that he has received the PIN envelope intact.

13.1.25 E-bank Users are required to use both the chip card and the PIN code to prove their authority when using the services.

13.1.26. The Bank shall have a new chip card manufactured prior to the expiry of the existing chip card subject to the fee published in the Announcement, unless the Client sends a written notice to the contrary by no later than 45 days before the expiry date of the current chip card. If the Client gives such instructions later, any costs resulting therefrom shall be borne by the Client.

13.1.27. When the new chip card is collected, any outstanding payments must be settled and the expiring chip card must be returned to the Bank.

13.1.28. If a technical fault occurs in a chip card, the e-bank User may apply for a replacement card. The Bank shall have the right to reject such an application without an explanation. If the technical fault of the card is attributable to improper use by the e-bank User, the Bank shall charge the fee published in the Announcement for the replacement card.

13.1.29. The Bank reserves the right to shut down the system for short periods from time to time for maintenance purposes. The Bank undertakes to inform the e-bank User about the likely downtime via the system. The Bank shall accept no liability for any damages resulting from such downtimes.

13.1.30. The Bank shall send its written notices to the Client to their correspondence address/registered office specified in the Contract, and by email. The Bank shall accept no liability for the failure of the Client to receive such written/electronic notices and the damages arising therefrom.

13.1.31. All e-bank Users shall have the same access rights to K&H corporate e-banking services. If the Contract is amended, the Parties shall monitor the access rights in force; if an inconsistency still exists, the Bank shall take into account the access rights recorded in the last order.

13.1.32. OPERATION IN PUBLIC PLACES

In public places the e-bank User shall take care to use the chip card reader required for the service and owned by the Bank normally, keeping it undamaged. The operator and the e-bank User shall be jointly and severally liable for any damages occurring in the chip card reader on such occasions. The fee payable therefor is published in the Announcement. In public places the e-bank User shall use the chip card reader according to the installation guide provided by the Bank to the operator and to comply with the requirements set out therein.

The Bank reserves the right to stipulate further requirements concerning the use of the chip card reader in public places both to the operator and the e-bank User.

The e-bank User acknowledges that the operator, pursuant to its legal relationship with the Bank, must immediately notify the Bank about any damage or fault occurring in the chip card reader or its loss, theft or any other events related thereto.

The Bank shall not be responsible for events and non-performances arising from the improper use of the chip card reader by the e-bank User.

The e-bank User acknowledges that the operator shall covenant under its legal relationship with the Bank to make every reasonable effort to identify any unauthorised uses of the services, and it shall have the system supervised by system managers twenty four hours, seven days. The Bank shall not check the e-bank User's authority to use the chip card reader or the circumstances of its use. The operator shall be solely liable for any damages arising from the unauthorised use of the chip card and this liability cannot be transferred to the Bank.

The above provisions shall also apply if the e-bank User fails to use the service with the specified banking tools.

13.2. SPECIAL PROVISIONS APPLICABLE TO K&H RETAIL TELEPHONE BANKING SERVICES

13.2.1. The K&H Retail Telephone Banking Services provides banking services to natural persons.

13.2.2. Transactions executed via the K&H Retail Telephone Banking Service and their fees shall be governed by the provisions of the Announcements concerning the bank accounts, deposit accounts and term deposits of natural persons and the Announcement concerning investment services and securities dealings.

13.3. SPECIAL PROVISIONS APPLICABLE TO K&H SME TELEPHONE BANKING SERVICES

13.3.1. K&H SME Telephone Banking Services comprise banking services specified in the General Contracting Terms and Conditions for account management, deposit and lending services provided by the Bank to businesses.

13.3.2. Clients may specify or modify the access rights of their authorised Transacting Persons in the relevant Annex to the Contract.

13.3.3. Each Querying/Transacting Person can query all the accounts of the Client without restrictions or limitations. However, transaction orders can only be given by Transacting Persons authorised by the Client.

13.3.4. A Transacting Person can modify or terminate their own access right to Banking Services Requiring Electronic Authentication in a telephone call to the K&H SME Telephone Banking Service.

13.3.5. The termination of a Transacting Person's access right to Banking Services Requiring Electronic Authentication may be initiated by the Transacting Person themselves (by telephone or in writing) or by the Client. The Client shall only exercise this right in writing via a branch clerk. The Transacting Person's instructions shall be accepted by the Bank until the day on which the Client terminates their access right.



13.3.6. If the Client fully terminates the access rights of all Transacting Persons, then only the Client shall be authorised to act via a branch clerk until the new Transacting Person(s) are appointed.

13.3.7. The Transacting Person shall not have the right:

- to transfer to others their signatory right pertaining to an account included in the scope of Banking Services Requiring Electronic Authentication;
- to collect bank account statements; and
- to sign, amend or terminate contracts for services outside the scope of Banking Services Requiring Electronic Authentication.

13.4. SPECIAL PROVISIONS APPLICABLE TO K&H CORPORATE TELEPHONE BANKING SERVICES

13.4.1. K&H Corporate Telephone Banking Services are services provided to Clients of the Bank that are resident or non-resident legal or unincorporated entities, organisations (foundations, churches, associations, municipalities etc), businesses or private individuals engaging in commercial activities by telephone whose scope is determined in the prevailing Announcement and particularly includes the provision of information, and general help, complaint management and advice concerning the corporate products of the Bank as well as taking instructions.

13.4.2. The Telephone Representative has the right to modify the access rights of Users linked to the accounts of the Client. The Telephone Representative has the right to terminate the relationship between the Users of the Client having appointed them and the K&H Corporate Telephone Banking Service.

13.4.3. The e-PIN code may be deleted at the express request of its holder or in the cases defined in Section 8.4.

13.4.4. The termination of a Telephone Representative's access rights may be initiated by the Telephone Representative themselves (by telephone or in writing) or by the Client. The Client shall only exercise this right in writing via its relationship manager. The instructions of the Telephone Representative shall be accepted by the Bank until the day on which the Client terminates their access right, after which only the Client shall be authorised to act via its relationship manager until a new Telephone Representative is appointed.

13.5. SPECIAL PROVISIONS APPLICABLE TO ELECTRA SERVICES

GENERAL PROVISIONS

13.5.1. Under the Electra service (hereinafter: the Service), the Electra User may take the following actions electronically in the currency defined in the Announcement:

- (a) give orders and notices to the Bank,
- (b) perform bank account statement queries of his account balance and turnover,
- (c) gain access to the current day currency/FX exchange rates of the Bank and to the FX exchange rates of the National Bank of Hungary.

13.5.2. The electra User may only perform Electronic Banking Operations for the execution of which the submission of documents by the Client or a third person and the inspection of the documents by the Bank or a third person are necessary pursuant to the Contract or legal regulations, subject to the prior fulfilment of these obligations.

13.5.3. For the purposes of Electronic Banking Operations performed by electra Users, the time established by the computer system of the Bank shall be regarded as the time of receipt of the

order or the notice by the Bank.

- 13.5.4. The Bank may limit the scope and the amount of Electronic Banking Operations in the Announcement.
- 13.5.5. In the future, the Bank may allow electra Users the performance of other Electronic Banking Operations. The Bank shall notify electra Users of such changes.
- 13.5.6. For the purpose of the written notices relating to the Service, the Bank shall provide electra Users with Forms. The Bank shall only accept written communications of the electra Users to the Bank as valid notices if submitted on these Forms.
- 13.5.7. Certain sub-services provided by the Bank under the Service (e.g.: installation, error elimination) may also be provided to electra Users with the involvement of an expert third person.
- 13.5.8. The rate of the bank costs charged for the Service shall be determined in the relevant Announcement of the Bank. Should the Contract stipulate bank costs different from the ones defined in the Announcement, the rates defined in the Contract shall apply.
- 13.5.9. The Bank shall also notify the electra User directly through the Electra System of any changes if the Service or any condition relating to the Service justify such notification or if the electra User and the Bank so agreed in this regard.

13.5.10. SPECIAL FEATURES OF THE SERVICE

Basic services:

- Client side administration
- Installation by the Client
- Information on the Bank's currency/FX exchange rates and on the FX exchange rates of the National Bank of Hungary
- Electronic bank account statement query service
- Current account balance
- Query on performed daily transactions
- Account history query
- Credit data query
- Exporting and importing of data in a certain format
- Encrypted data transmission between the Bank and the Client (acountholder)
- Submission of HUF and FX transfers, HUF internal transfers from HUF and FX accounts
- VIBER transfers from HUF accounts
- Submission of collection orders
- Opening and termination of term deposits
- Management of authorizations
- Hungarian, English and German Electra menus
- On-line help
- Standing transfers
- Saving, archiving of data
- Management of data of partners

Supplementary services:

- Submission of group transfer orders, receipt of DETSTA and STATUSZ reports
- Submission of group collection orders, receipt of DETSTA and STATUSZ reports

- Submission of postal payment orders, receipt of postal identification data
- Receipt of data of postal cash transfer orders
- Urgent transfers (on T-day)

INSTALLATION, PUTTING INTO OPERATION OF ELECTRA

13.5.11. The Electra service is installed by the Client himself using the installation toolkit, which can be downloaded from the Bank's website and an installation code sent to the Client by SMS with the help of the group code, user name and Token specified on the data sheet. In other cases – if the Client specifically requests bank administration or requests cooperation from the Bank in the case of choosing Client side administration, the Electra service is installed by the Bank at the site specified by the Client – against the fee defined in the Announcement. In the case of installation by the Bank, the Bank shall also provide training on the use of the installed system. The Client shall confirm the contractual installation of the Electra Software by the Bank by signing the Installation Record.

ACCESS RIGHTS:

13.5.12. The Client defines the authorized persons and the scope of their access rights in respect of the Electra service for the Bank on the relevant Annex.

In the case of Client side administration, the access right may cover the following:

- query right specified for each account,
- query right for all accounts,
- signature right specified for each account.

In the case of bank administration, the access right may extend to the following:

- query right specified for each account,
- query right for all accounts,
- signature right specified for each account,
- signature right not relating to an account (company level signature right) and
- group right defined as a group authentication.

13.5.13. Electra Users having either only query rights or other rights as well may use their rights after providing their Token passwords.

13.5.14. The electra User having query rights for all accounts may perform queries of every account of the Client. The scope of this query right automatically extends to newly opened accounts also for which the query right of the User is set automatically. To modify rights, the Client shall set the appropriate authorizations himself in the case of Client side administration. In the case of Bank administration, the appropriate authorizations shall be requested for the new account on a data sheet.

13.5.15. Signature rights shall be defined for each User with the help of a score (of 1 to 10 points). The Bank shall only accept the orders signed with 10-point authorization. For the submission of orders, signature rights defined for specific accounts have to be defined in the case of current accounts. A signature right not related to accounts is required at the time of the software installation for the registration of the client program and also for the termination of term deposits, for the confirmation of authorizations relating to group collection orders and, in the

case of Client side administration, for the administration of the registration of additional users.

13.5.16. Regarding the definition of authorizations, it is the Client's responsibility to determine the person or persons who are authorized to use the Electra System installed at the Client. The Bank and the Electra System shall regard those persons as authorized who have been registered by the Client in the case of Client side administration or who have been reported to the Bank as such on the form provided by the Bank in the relevant Annex. The user authorization levels specified this way shall only apply to the Electra client terminal.

13.5.17. The Bank shall set centrally:

- in the case of Client side administration: the authorizations of the first two Users.
- in the case of Bank side administration: the authorizations of the Users specified by the Client.

The User shall define his Token password at the time of the first registration. In the case of Users having signature rights, the same code will qualify as the code required for the approval, confirmation of specific orders.

13.5.18. The electra User shall ensure that no other person has access to his Token password. The Bank shall not be liable for damages arising from unauthorized use.

13.5.19. The User acknowledges that if he enters his Token password incorrectly for five times in succession, he shall automatically lose access to the Electra service for the future.

13.5.20. In the event defined in Section 13.5.20, the User shall release the blocked Token password himself with the help of the Bank's Telephone Banking Services for which the e-PIN code is required.

13.5.21. The Client shall notify and consult the Bank in advance if he intends to modify his hardware or software system.

RECEIPT AND EXECUTION OF ORDERS

13.5.22. The deadline for the receipt by the Bank of the Orders to be executed on the current day is specified in the Announcement.

13.5.23. The Client/User shall regularly save the computer files containing his orders and notices to magnetic data carriers or CD-s and store these (with the exception of CD-s) in a safe place free of magnetic effects. The Client shall keep the files saved in this manner for a period of at least 30 working days.

13.5.24. The Bank shall regard as valid orders only the orders submitted to it by the User, which were found formally correct by the Electra System and which also complied fully with provisions of legal regulations and of the Contract in terms of content.

13.5.25. The Bank shall be entitled to debit the account in accordance with the orders which were placed using the Token password.

BLOCKING, REPORTING OBLIGATION OF USERS

13.5.26. Blocking, in the case of Client side administration, is performed by the Client (or other User) himself with the help of the Electra terminal or by phone with the help of the Bank using the e-PIN code.

13.5.27. In the case of Bank side administration: The User shall report the following events immediately upon being informed of them by calling the phone number defined in the Contract (available 24

hours a day, every day of the year):

- (a) receipt of the Token password by unauthorized persons, and
- (b) loss or theft of the Token

(c) indication of an unauthorized operation on the Client's bank account statement due to which the Client requests (in the case of the Electra Software) the blocking of the Service or the blocking of any User.

- 13.5.28. The reporting of the above listed events must contain the Client's company name, registered seat, tax number, account number, the accurate definition of the event reported, the name of the reporting person and a fax/phone number at which the Bank can confirm the reported event as well as a declaration that the reporting person expressly requests, in the case of the Electra Software, the blocking of the entire Service or a specific User. In the event defined in Section 9.1 b), if the reporting person does not request blocking at the time of reporting the event, the Bank shall proceed in accordance with the rules pertaining to complaints.
- 13.5.29. The Bank shall execute blocking immediately during the phone-call in the case of events reported between 7.00 AM and 5.00 PM on banking days. In the case of events reported on holidays and between 5.00 PM and 7.00 AM on banking days, the Bank shall execute the blocking before the processing of the payment items received after 5.00 PM on the previous banking day.
- 13.5.30. Within one hour of the blocking but on the next banking day at the latest, the Bank shall confirm the event reported and the blocking by sending a fax message to the fax number specified by the reporting person.
- 13.5.31. An event is considered reported if the reporting person has provided all of the data requested by the Bank (with the exception of only the tax number). The blocking shall become effective when the Bank has taken the measures required for the blocking within a reasonable time necessary these measures. The Bank shall record the time of reporting in accordance with the local time applied in the Bank's systems.
- 13.5.32. The Client shall bear the risk of blocking and all damages arising from the fact that the blocked Token password cannot be used. The Bank shall assume no liability for damages suffered by either the User or by any third person due to the failure to block the Token password or an abuse relating to the blocking process.
- 13.5.33. If the damage arising from unauthorized use was not caused by an intentional behaviour or gross negligence of the User, the User shall cover the damage arising before the reporting and the request of blocking of the Token password up to the amount of HUF 45,000.
- 13.5.34. The Bank shall keep a record of the events reported. Upon the request of the Client, the Bank shall issue a certificate of the fact that an even was reported and on the content and time of the report made retroactively for a period of maximum five years.
- 13.5.35. Any damages arising between the time of being informed of the fact forming the basis of the reporting and the time of reporting of this fact to the Bank shall be borne by the Client.
- 13.5.36. The Bank shall be liable for the damages arising after the reporting of the relevant event unless the damage arising after reporting is caused by the User himself by an intentional or grossly negligent breach of contract.
- 13.5.37. If, based on a judgment of facts with the generally expected care, a criminal act has taken place, the Client (or other User) shall immediately report this suspicion to the authority competent for

the investigation of criminal acts.

13.5.38. The blocking of the Token password is final and irrevocable. The Service may not be used from the time of confirmation until the release of blocking. The blocking may be released by the representative of the Client personally at the account managing branch by filling out the Form received at the branch and signing it in the corporate signature registered with the Bank.

13.5.39. The costs arising at the Bank and at the Client in relation to the blocking of the Token password shall be borne by the Client.

LIABILITY

13.5.40. The Bank shall not be liable for the damages arising from errors of the Electra Software, the inappropriate transmission of data, incorrect or incomplete data or non-updated information unless such damages can be proven to have occurred due to an error of the Bank. Also, the Bank reserves the right to interrupt the availability of the system on an occasional basis (due to system maintenance) for a short time. The Bank shall notify the electra User of the expected time of the interruption through the system. The Bank shall not be liable for damages potentially arising from such interruptions.

13.5.41. The Bank shall only be obliged to restore the Client's data if such data can be proven to have been corrupted or destroyed due to a software error caused by the Bank provided that the Client took measures to ensure that the data can be restored from materials stored in a format readable by the Electra System.

13.5.42. The Client shall cover all damages arising from the inappropriate use of the Tokens provided to the Users or the use of the Tokens by an unauthorized person. The only exemption from this rule shall be the damages arising after the reporting of the Token or, in the case of the Electra Software, the Service to the Bank.

13.5.43. The Client shall be liable towards the Bank and other collaborators for all damages arising from the fact that the orders placed by the User or the data provided by the user were inappropriate, incorrect or incomplete.

13.5.44. The Bank shall not be liable for damages arising from the fact that the instruction (order) of the User is damaged, become uninterpretable or is made available to unauthorized persons during data transmission due to incorrect or failing operation of the modem or data transmission connection. The Bank shall have no liability for damages arising from the manipulation of the data files by any person during data transmission.

13.5.45. The User shall use the Electra Software at the risk and liability of the Client and may connect the computer to the Bank's Electra System at the liability of the Client. Accordingly, the Bank's liability shall not be grounded on damage to the Client's computer or the data files stored on the Client's computer or damage to other peripherals, computers, software or data files connected to the Client's computer caused by the Electra Software or the Electra System or an error or breakdown of the Electra Software or the Electra System or any other damage arising from the fact that the Client is not authorized to dispose of the computer appointed for the installation of the Electra Software.

ELECTRA SOFTWARE, AUTHORIZATIONS

13.5.46. Each module of the Electra Software is the exclusive property of the licensor of the Bank and each item of the Electra Software and each authorized copy made of the Electra Software is and shall remain the property of the licensor of the Bank. All intellectual property rights,

copyrights, trademarks and secrets relating to the Electra Software are and shall remain the property of the Bank and the licensor of the Bank. The Client (User) has no right to sell, transfer, publish, dispose of, communicate and in general to make any item or any copy of the Electra Software available to third parties unless authorized to do so by the Bank in writing.

- 13.5.47. The Bank grants the Client or the User the right to use the Electra Software, which may only be run subject to the hardware criteria and on the operating system defined in this GCTC. The Client shall always use the latest version of the Electra Software provided by the Bank, which shall either be updated online or the current updates may be downloaded from the Bank's internet portal and installed on the Client's computer.
- 13.5.48. The right to use the Electra Software is granted to the Client on a non-exclusive basis and subject to a transfer ban. The Electra Software shall be used under the Client's exclusive liability in compliance with the provisions applicable to the use of the Electra Software.
- 13.5.49. The right to use the Electra Software is expressly limited to the delivered "binary code". The Client may not attempt to reconstruct the "source" of the Electra Software or reconstruction from any other element included in the Electra Software (by way of disassembly, de-compilation or in any other manner).
- 13.5.50. The Client shall not have the right to make a "back up" of the Electra Software. The Client has no right to modify the Electra Software, to combine it with other software unless expressly authorized to do so. If such an authorization exists, the Client shall bear all and any risk arising from the modification with special regard to the risk of incompatibility which may arise between the modified Electra Software and any hardware, software or future software, software version, software update, test, diagnostic or control routine.
- 13.5.51. The Bank shall grant the right of use for a period starting on the day of delivery of the Electra Software and ending when the Client terminates the use of the Service or the Contract concluded between the Parties terminates for any other reason.
- 13.5.52. If the Client fails to comply with any of the obligations defined in the Contract regarding the use of the Electra Software, the Bank shall be entitled to immediately withdraw the right of use in respect of each item of the Electra Software without any special legal procedure.
- 13.5.53. The Client hereby obliges to take any necessary measures in order to protect the rights of the Bank or the licensor of the Bank from violations by the Client's own employees and representatives or any other person who may have access to the documentation, the Electra Software and the know-how.
- 13.5.54. In the case of failure to comply with the above obligation, the Client shall bear full liability for all legal consequences and for the breach of the Contract including the obligation to indemnify and damage caused.
- 13.5.55. The Client shall destruct the Electra Software within one day of the day of termination of his right of use for any reason and send a written declaration to the Bank of the destruction of the software.

ELECTRA SOFTWARE WARRANTY

- 13.5.56. The Bank warrants that the Electra Software complies with the specifications communicated by the Bank at the time of delivery and it can be used properly on the contractual hardware and operating system. In the case of installation by the Bank, the Bank shall install the Electra System and train one person acting on behalf of the Client to use the Electra System at the site

of installation within a maximum of 2 hours.

13.5.57. The warranty of the Bank shall not extend to the peripheries of the hardware containing the Electra Software and any hardware and software connected to the Electra Software.

13.5.58. The Client acknowledges that the Bank may use the services of expert third persons for the installation of the Electra Software and the fulfilment of its obligations under the warranty.

13.5.59. The warranty service of the Electra Software covers the following:

- (a) advisory service in relation to the installation of the Electra Software Module, the updates and corrections provided and authorized by the Bank,
- (b) advisory service for the identification of errors,
- (c) advisory service for the solution of the problems arising during the installation of the updates and corrections,
- (d) elaboration of temporary corrections or alternative solutions,
- (e) investigation of reports on problems,
- (f) delivery of updates.

13.5.60. As a precondition to the provision of the Electra Software warranty service the Client undertakes to provide access to the Electra Software and the hardware containing the Electra Software under the conditions requested by the Bank and for the time required to provide the warranty service during the entire term of the Contract. The Client shall always use the latest Electra Software version provided by the Bank.

13.5.61. Services beyond the scope of the Electra Software warranty:

- solution of the problems arising from non-contractual or non-documented use of the Electra Software or negligence,
- regeneration of the Electra Software in the cases when regeneration is not necessary due to an error for which the Bank is accountable,
- modification of the functions of the Electra Software upon the Client's request.

TERMINATION OF SERVICE

13.5.62. If the Client does not use any Electra Software Module (does not log on to the Electra client program) for a period of at least 6 months), the Bank may delete the Electra Software Module not used from the Electra System. If the Client does not use the Electra Software Module (or, in the case of more than one Electra Software Modules, all of the modules) for more than one (1) year, the Bank may terminate further access of the Client to the Electra System, which shall imply automatic termination of the Contract.

13.5.63. In the case of termination of the Contract for any reason, the fees, commissions and costs not paid to the Bank shall become due and payable in one lump sum on the day of termination.

13.6. SPECIAL PROVISIONS APPLICABLE TO K&H E-BOX SERVICES

13.6.1. The K&H e-box service is available to the Users of the non-natural-person Clients, which have a valid and effective contract in place with the Bank for the products defined in the relevant Announcement and have the hardware and software instruments required for the use of the service, which are listed in the user manual.

- 13.6.2. The e-box User must have and be authorized to use the equipment defined by the Bank as necessary for the use of the K&H e-box service. The e-box User shall familiarize himself with the technical attributes and the proper use of these equipment and other tools necessary for the use of the service. The Bank shall not assume liability for damages arising from improper use.
- 13.6.3. The Bank shall – based on the User's needs – provide the e-box User with the authentication tools and equipment required for the use of the services (the property of the Bank) and the installation guide demonstrating their use. The authentication tool is the property of the Bank and the e-box User as its holder shall only be given it for use. The user manual and the installation guide for the services and the driver for the chip card reader can be downloaded from <https://ebank.khb.hu/>. The Bank reserves the right to update and supplement the user manual from time to time in order to improve the quality of the service and develop the applications. The update of the user manual shall not constitute an amendment of the Contract under any circumstances, and the Bank shall inform e-box Users thereof electronically through the internet using the e-box application.
- 13.6.4. Regarding the definition of access rights in the case of the K&H e-box service, it is the Client's exclusive responsibility to determine the person or persons who are authorized to use the service. For the purpose of the execution of electronic banking operations, the Bank shall regard those persons as legitimate e-box Users who have been reported to the Bank as such on the form provided by the Bank in the relevant Annex.
- 13.6.5. The Bank sets e-box User authorizations on the basis of the authorizations reported by the Bank and produces the authentication tools to be provided personally to the given e-box Users.
- 13.6.6. The Client may request from the Bank the cancellation of the access rights of a certain e-box User or the modification of user data in writing on the form provided the relevant Annex of.
- 13.6.7. The Bank reserves the right to interrupt the availability of the system on an occasional basis (due to system maintenance) for a short time. The Bank shall notify the e-box User of the expected time of the interruption. The Bank shall not be liable for damages potentially arising from such interruptions.